CLAIMS

I/we claim:

1. A method of producing a response with a device comprising an input (2) for receiving an input (INPUT);

calculation means (P, P', P'') for producing a response (OUTPUT) which is responsive to the input and a secret key (A) by utilizing a first predetermined function (f), and

an output (3) for feeding said response (OUTPUT) further, characterized by

storing in a memory (M', M'') of the device a key-specific number (RND) and a coded key (A'), which is calculated by means of the secret key (A), the key-specific number (RND) and a second predetermined function (g), and,

when producing the response (OUTPUT),

reading said key-specific number (RND) and coded key (A') from the memory,

calculating the secret key (A) on the basis of said key-specific number (RND) and coded key (A') by using the inverse function (g') of said second predetermined function (g), and

utilizing the calculated secret key (A) to produce said response (OUTPUT).

2. The method as claimed in claim 1, characterized in that said second predetermined function (g) is a device-specific function, and that said key-specific number (RND) is a random number.

3. The method as claimed in claim 1, characterized by calculating and storing in the memory (M'') of the device (1'') a new coded key (A') and a new key-specific number (RND), when the calculation means (P'') have utilized said first predetermined function (f) a predetermined number of times.

4. The device (1, 1', 1'') comprising

an input for receiving an input;

calculation means (P, P', P'') for producing a response (OUTPUT) which is responsive to the input (INPUT) and a secret key (A) by utilizing a first predetermined function (f), and

an output (3) for feeding said response (OUTPUT) further, characterized by further comprising

a memory (M, M', M'') for storing a key-specific number (RND) and a coded key (A'), which is calculated by means of the secret key (A), the key-specific number (RND) and a second predetermined function (g), and

means for retrieving the key-specific number (RND) and the coded key (A') from the memory (M, M', M'') and feeding them to the calculation means (P, P', P''), which calculate the secret key (A) by means of the coded key (A'), the key-specific number (RND) and the inverse function (g') of said second predetermined function (g) when producing said response (OUTPUT).

5. The device as claimed in claim 4, characterized in that the device (1'') comprises coding means (5'') for calculating a new coded key (A') by means of the secret key (A), a new key-specific number (RND) to be fed to the coding means, and said second predetermined function (g), and that the device (1'') comprises means for replacing the coded key (A') and the key-specific number (RND) stored in the memory (M'') with the new coded key (A') calculated by the coding means (5''), and the new key-specific number (RND).

6. The system comprising

a device (1, 1', 1'') having an input for receiving an input (INPUT), calculation means (P, P', P'') for producing a response (OUTPUT) which is responsive to the input (INPUT) and a secret key (A) by utilizing a first predetermined function (f), and an output for feeding said response further, and

an apparatus (10, 10'), which is connected to the input of the device (1, 1', 1'') for feeding said input (INPUT) to the device, and to the output of the device for receiving said response (OUTPUT), said apparatus (10, 10') further comprising a memory (M2) for storing said secret key (A), calculation means (P2) for calculating a check value by means of the input (INPUT), the secret key (A) and said first predetermined function (f), and means (12), which compare the response (OUTPUT) obtained from the output of the device (1) with the check value and indicate if the response corresponds to the check value, characterized in that the device (1, 1', 1'') further comprises

a memory (M, M', M'') for storing a key-specific number (RND) and a coded key (A'), which is calculated by means of the secret key (A), the key-specific number (RND) and a second predetermined function (g), and

means for retrieving the key-specific number (RND) and the coded key (A') from the memory (M, M', M'') and for feeding them to the calculation means (P, P', P''), which calculate the secret key (A) by means of the coded key (A'), the key-specific number (RND) and the inverse function (g') of said second predetermined function (g) when producing said response (OUTPUT).

7. The system as claimed in claim 6, characterized in that said apparatus (10') comprises

means for calculating the coded key (A') by means of the secret key (A), the key-specific number (RND) and the second predetermined function (g), and

means for storing the coded key (A') and the key-specific number (RND) in the memory (M') of the device (1').

8. The system as claimed in claim 7, characterized in that said apparatus (10') further comprises a random number generator (13) for generating the key-specific number (RND) during the calculation of the coded key (A').